CLAIMS

1. In a computer system comprising a plurality of nodes interconnected for communication via a network, a method including acts of:

(A) capturing, in a data structure, a notification provided by a node on the network, the notification comprising at least a portion of a transmission by the node, the transmission describing a network event;

(B) identifying a data element within the notification;

(C) updating an index, based on the data element, with an indication of a location within the data structure where the data element is recorded.

2. The method of claim 1, wherein the act (A) further comprises storing the data structure in a non-volatile storage.

3. The method of claim 2, wherein the act (A) further comprises storing the data structure in a file system in the non-volatile storage.

4. The method of claim 3, wherein the file system is a hierarchical file system.

5. The method of claim 3, further comprising an act comprising classifying the notification based on the data element, and wherein the act (A) further comprises storing the data structure in the file system based on the classification.

6. The method of claim 5, wherein the data element comprises an IP address of the node.

7. The method of claim 1, wherein the data structure is a file.

8. The method of claim 2, further comprising an act of compressing the data structure.

9. The method of claim 2, further comprising an act of creating a digital signature for the data structure.

10. The method of claim 1, wherein the transmission comprises at least one of a SYSLOG message, an SNMP message, a NetFlow message and a TCP packet.

11. The method of claim 1, further comprising acts of:

(D) accessing the index to determine, based on the indication, the location of the data element within the data structure; and

(E) accessing the data element at the location.

12. The method of claim 1, further comprising an act of creating a summary based at least in part on a presence of the data element within the notification.

13. The method of claim 12, further comprising an act comprising accessing the summary to determine the presence of the data element within the data structure.

14. At least one computer-readable medium encoded with instructions which, when executed by a computer, perform a method in a computer system comprising a plurality of nodes interconnected for communication via a network, a method including acts of:

(A) capturing, in a data structure, a notification provided by a node on the network, the notification comprising at least a portion of a transmission by the node, the transmission describing a network event;

(B) identifying a data element within the notification;

(C) updating an index, based on the data element, with an indication of a location within the data structure where the data element is recorded.

15. The at least one computer-readable medium of claim 14, further comprising instructions defining storing the data structure in a non-volatile storage.

16. The at least one computer-readable medium of claim 15, further comprising instructions defining storing the data structure in a file system in the non-volatile storage.

17. The at least one computer-readable medium of claim 16, wherein the file system is a hierarchical file system.

18. The at least one computer-readable medium of claim 16, further comprising instructions defining classifying the notification based on the data element and storing the data structure in the file system based on the classification.

19. The at least one computer-readable medium of claim 18, wherein the data element comprises an IP address of the node.

20. The at least one computer-readable medium of claim 14, wherein the data structure is a file.

21. The at least one computer-readable medium of claim 15, further comprising instructions defining compressing the data structure.

22. The at least one computer-readable medium of claim 15, further comprising instructions defining creating a digital signature for the data structure.

23. The at least one computer-readable medium of claim 14, wherein the transmission comprises at least one of a SYSLOG message, an SNMP message, a NetFlow message and a TCP packet.

24. The at least one computer-readable medium of claim 14, further comprising instructions defining accessing the index to determine, based on the indication, the location of the data element within the data structure; and accessing the data element at the location.

25. The at least one computer-readable medium of claim 14, further comprising instructions defining creating a summary based at least in part on a presence of the data element within the notification.

26. The at least one computer-readable medium of claim 25, further comprising instructions defining accessing the summary to determine the presence of the data element within the data structure.

27. A system for monitoring activity occurring in a computer system comprising a plurality of nodes interconnected for communication via a network, the system comprising:

a capture controller, said capture controller capturing, in a data structure, a notification provided by a node on the network, the notification comprising at least a portion of a transmission by the node, the transmission describing a network event;

an identification controller, said identification controller identifying a data element within the notification;

an update controller, said update controller updating an index, based on the data element, with an indication of a location within the data structure where the data element is recorded.

28. The system of claim 27, wherein the capture controller further stores the data structure in a non-volatile storage.

29. The system of claim 28, wherein the capture controller further stores the data structure in a file system in the non-volatile storage.

30. The system of claim 29, wherein the file system is a hierarchical file system.

31. The system of claim 29, further comprising a classification controller, said classification controller classifying the notification based on the data element, wherein the capture controller stores the data structure in the file system based on the classification.

32. The system of claim 31, wherein the data element comprises an IP address of the node.

33. The system of claim 27, wherein the data structure is a file.

34. The system of claim 28, further comprising a compression controller, said compression controller compressing the data structure.

35. The system of claim 28, further comprising a signature controller, said signature controller creating a digital signature for the data structure.

36. The system of claim 27, wherein the transmission comprises at least one of a SYSLOG message, an SNMP message, a NetFlow message and a TCP packet.

37. The system of claim 27, further comprising:

an access controller, said access controller accessing the index to determine, based on the indication, the location of the data element within the data structure; and accessing the data element at the location.

38. The system of claim 27, further comprising a summary controller, said summary controller creating a summary based at least in part on a presence of the data element within the notification.

39. The system of claim 38, further comprising a summary access controller, said summary access controller accessing the summary to determine the presence of the data element within the data structure.

40. A method for monitoring activity on a networked computer system, the networked computer system comprising a plurality of nodes, each of the plurality of nodes configured to transmit a notification for each event processed by the node, the networked computer system further comprising a plurality of sites, each of the plurality of sites being configured to capture the notifications transmitted by at least one node, the method comprising:

(A) each of the plurality of sites creating an indication of the notifications captured by the site;

(B) each of the plurality of sites transferring the indication to at least one other of the plurality of sites.

41. The method of claim 40, wherein the plurality of sites are organized into a hierarchy, wherein each site in the hierarchy is assigned at least one of a master site and a subordinate site.

42. The method of claim 41, wherein each site performs at least one transfer of an indication, wherein the at least one transfer is performed to at least one of a subordinate site and a master site.

43. The method of claim 42, wherein each site performs a transfer to its master site and receives a transfer from its master site, and wherein as a result of the transfers, each site receives the indication created by each other site.

44. The method of claim 43, further comprising acts of:

(C) receiving, by a site, a query requesting information on an event processed by a node from which the site does not capture notifications; and

(D) processing the query, by the site, by accessing at least one indication transferred to the site by another site.

45. The method of claim 44, further comprising acts of:

(E) determining, by the site, based on the at least one indication transferred to the site by another site, that the at least one indication does not contain the information requested by the query;

(F) identifying, by the site, which of the other sites may have captured the information requested by the query;

(G) creating, by the site, at least one additional query requesting the information from at least one other site identified in the act (F); and

(H) transmitting, by the site, the at least one additional query to the at least one other site.

46. The method of claim 45, further comprising acts of:

(I) receiving, at the site, a response for each of the at least one additional queries from the at least one other site; and

(J) aggregating, by the site, the responses received.

47. The method of claim 40, wherein the act (A) further comprises creating, by each of the plurality of sites, an indication which includes a representation of data stored in a file system on the site.

48. The method of claim 40, wherein each site captures notifications transmitted by nodes deployed in a geographic area.

49. The method of claim 40, wherein each site captures the notifications transmitted by a set of nodes, the set of nodes remaining unchanged.

50. The method of claim 40, wherein the plurality of sites comprises two portions, wherein a first portion includes sites configured to communicate with any other site in the first portion, and wherein a second portion includes at least one site configured to communicate with only one site in the first portion, the method comprising acts of:

(A) capturing, by a site in the second portion, an indication of the notifications captured by the site;

(B) transferring, by the site in the second portion, the indication to a site in the first portion.

51. The method of claim 50, further comprising an act of:

(C) transferring, by the site in the first portion, the indication to another site in the first portion.

52. The method of claim 50, wherein the act (B) is performed after a predetermined period of time elapses.

53. The method of claim 50, wherein the act (B) is performed after a notification captured by the site in the second portion satisfies a predetermined criterion.

54. At least one computer-readable medium encoded with instructions which, when executed by a computer, perform a method for monitoring activity on a networked computer system, the networked computer system comprising a plurality of nodes, each of the plurality of nodes configured to transmit a notification for each event processed by the node, the networked computer system further comprising a plurality of sites, each of the plurality of sites being configured to capture the notifications transmitted by at least one node, the method comprising:

(A) each of the plurality of sites creating an indication of the notifications captured by the site;

(B) each of the plurality of sites transferring the indication to at least one other of the plurality of sites.

55. The at least one computer-readable medium of claim 54, wherein the plurality of sites are organized into a hierarchy, wherein each site in the hierarchy is assigned at least one of a master site and a subordinate site.

56. The at least one computer-readable medium of claim 55, further comprising instructions defining each site performing at least one transfer of an indication, wherein the at least one transfer is performed to at least one of a subordinate site and a master site.

57. The at least one computer-readable medium of claim 56, further comprising instructions defining each site performing a transfer to its master site and receiving a transfer from its master site, wherein, as a result of the transfers, each site receives the indication created by each other site.

58. The at least one computer-readable medium of claim 57, further comprising instructions defining:

(C) receiving, by a site, a query requesting information on an event processed by a node from which the site does not capture notifications; and

(D) processing the query, by the site, by accessing at least one indication transferred to the site by another site.

59. The at least one computer-readable medium of claim 58, further comprising instructions defining:

(E) determining, by the site, based on the at least one indication transferred to the site by another site, that the at least one indication does not contain the information requested by the query;

(F) identifying, by the site, which of the other sites may have captured the information requested by the query;

(G) creating, by the site, at least one additional query requesting the information from at least one other site identified in the act (F); and

(H) transmitting, by the site, the at least one additional query to the at least one other site.

60. The at least one computer-readable medium of claim 59, further comprising instructions defining:

(I) receiving, at the site, a response for each of the at least one additional queries from the at least one other site; and

(J) aggregating, by the site, the responses received.

61. The at least one computer-readable medium of claim 54, further comprising instructions defining creating, by each of the plurality of sites, an indication which includes a representation of data stored in a file system on the site.

62. The at least one computer-readable medium of claim 54, further comprising instructions defining each site capturing notifications transmitted by nodes deployed in a geographic area.

63. The at least one computer-readable medium of claim 54, further comprising instructions defining each site capturing the notifications transmitted by a set of nodes, the set of nodes remaining unchanged.

64. The at least one computer-readable medium of claim 54, wherein the plurality of sites comprises two portions, wherein a first portion includes sites configured to communicate with any other site in the first portion, and wherein a second portion includes at least one site configured to communicate with only one site in the first portion, further comprising instructions defining:

(K) capturing, by a site in the second portion, an indication of the notifications captured by the site;

(L) transferring, by the site in the second portion, the indication to a site in the first portion.

65. The at least one computer-readable medium of claim 64, further comprising instructions defining:

(M) transferring, by the site in the first portion, the indication to another site in the first portion.

66. The at least one computer-readable medium of claim 64, further comprising instructions defining performing the act (L) after a predetermined period of time elapses.

67. The at least one computer-readable medium of claim 64, further comprising instructions defining performing the act (L) after a notification captured by the site in the second portion satisfies a predetermined criterion.

68. A system for monitoring activity on a networked computer system, the networked computer system comprising a plurality of nodes, each of the plurality of nodes configured to transmit a notification for each event processed by the node, the networked computer system further comprising a plurality of sites, each of the plurality of sites being configured to capture the notifications transmitted by at least one node, comprising:

a creation controller on each of the plurality of sites, said creation controller creating an indication of the notifications captured by the site;

a transfer controller on each of the plurality of sites, said transfer controller transferring the indication to at least one other of the plurality of sites.

69. The system of claim 68, wherein the plurality of sites are organized into a hierarchy, wherein each site in the hierarchy is assigned at least one of a master site and a subordinate site.

70. The system of claim 69, wherein each site performs at least one transfer of an indication, wherein the at least one transfer is performed to at least one of a subordinate site and a master site.

71. The system of claim 70, wherein each site performs a transfer to its master site and receives a transfer from its master site, and wherein as a result of the transfers, each site receives the indication created by each other site.

72. The system of claim 71, further comprising:

a receipt controller on a site, said receipt controller receiving a query requesting information on an event processed by a node from which the site does not capture notifications; and

a query controller, said query controller processing the query by accessing at least one indication transferred to the site by another site.

73. The system of claim 72, further comprising:

a determination controller, said determination controller determining, based on the at least one indication transferred to the site by another site, that the at least one indication does not contain the information requested by the query;

an identification controller, said identification controller identifying which of the other sites may have captured the information requested by the query;

a creation controller, said creation controller creating at least one additional query requesting the information from at least one other site identified by the identification controller; and

a transmission controller, said transmission controller transmitting the at least one additional query to the at least one other site.

74. The system of claim 73, further comprising:

a response controller, said response controller receiving a response for each of the at least one additional queries from the at least one other site; and

an aggregation controller, said aggregation controller aggregating the responses received.

75. The system of claim 68, wherein the creation controller on each of the plurality of sites further creates an indication which includes a representation of data stored in a file system on the respective site.

76. The system of claim 68, wherein each site captures notifications transmitted by nodes deployed in a geographic area.

77. The system of claim 68, wherein each site captures the notifications transmitted by a set of nodes, the set of nodes remaining unchanged.

78. The system of claim 68, wherein the plurality of sites comprises two portions, wherein a first portion includes sites configured to communicate with any other site in the first portion, wherein a second portion includes at least one site configured to communicate with only one site in the first portion, and wherein the system further comprises:

a remote collection controller on a site in the second portion, the remote collection controller capturing an indication of the notifications captured by the site;

a transfer controller, said transfer controller transferring the indication captured by the remote collection controller to a site in the first portion.

79. The system of claim 78, further comprising:

a local collection controller, said local collection controller transferring the indication received from the transfer controller to another site in the first portion.

80. The system of claim 78, wherein the transfer controller transfers the indication after a predetermined period of time elapses.

81. The system of claim 78, wherein the transfer controller transfers the indication upon a notification captured by the site in the second portion satisfying a predetermined criterion.

82. A system for monitoring activity occurring in a computer system comprising a plurality of nodes interconnected for communication via a network, the system comprising:

means for capturing, in a data structure, a notification provided by a node on the network, the notification comprising at least a portion of a transmission by the node, the transmission describing a network event;

means for identifying a data element within the notification;

means for updating an index, based on the data element, with an indication of a location within the data structure where the data element is recorded.

83. The system of claim 82, wherein the means for capturing stores the data structure in a non-volatile storage.

84. The system of claim 83, wherein the means for capturing stores the data structure in a file system in the non-volatile storage.

85. The system of claim 84, wherein the file system is a hierarchical file system.

86. The system of claim 84, further comprising means for classifying the notification based on the data element, wherein the means for capturing stores the data structure in the file system based on the classification.

87. The system of claim 86, wherein the data element comprises an IP address of the node.

88. The system of claim 82, wherein the data structure is a file.

89. The system of claim 83, further comprising means for compressing the data structure.

90. The system of claim 83, further comprising means for creating a digital signature for the data structure.

91. The system of claim 82, wherein the transmission comprises at least one of a SYSLOG message, an SNMP message, a NetFlow message and a TCP packet.

92. The system of claim 82, further comprising:

means for accessing the index to determine, based on the indication, the location of the data element within the data structure; and

means for accessing the data element at the location.

93. The system of claim 82, further comprising means for creating a summary based at least in part on a presence of the data element within the notification.

94. The system of claim 93, further comprising means for accessing the summary to determine the presence of the data element within the data structure.

95. A system for monitoring activity on a networked computer system, the networked computer system comprising a plurality of nodes, each of the plurality of nodes configured to transmit a notification for each event processed by the node, the networked computer system further comprising a plurality of sites, each of the plurality of sites being configured to capture the notifications transmitted by at least one node, comprising:

means for creating, on each of the plurality of sites, an indication of the notifications captured by the site;

means for transferring, on each of the plurality of sites, the indication to at least one other of the plurality of sites.

96. The system of claim 95, wherein the plurality of sites is organized into a hierarchy, and wherein each site in the hierarchy is assigned at least one of a master site and a subordinate site.

97. The system of claim 96, wherein each site performs at least one transfer of an indication, wherein the at least one transfer is performed to at least one of a subordinate site and a master site.

98. The system of claim 97, wherein each site performs a transfer to its master site and receives a transfer from its master site, and wherein as a result of the transfers, each site receives the indication created by each other site.

99. The system of claim 98, further comprising:

means for receiving a query requesting information on an event processed by a node from which the site does not capture notifications; and

means for processing the query by accessing at least one indication transferred to the site by another site.

100. The system of claim 99, further comprising:

means for determining, based on the at least one indication transferred to the site by another site, that the at least one indication does not contain the information requested by the query;

means for identifying which of the other sites may have captured the information requested by the query;

means for creating at least one additional query requesting the information from at least one other site identified by the identification controller; and

means for transmitting the at least one additional query to the at least one other site.

101. The system of claim 100, further comprising:

means for receiving a response for each of the at least one additional queries from the at least one other site; and

means for aggregating the responses received.

102. The system of claim 95, wherein the means for creating on each of the plurality of sites creates an indication which includes a representation of data stored in a file system on the respective site.

103. The system of claim 95, wherein each site captures notifications transmitted by nodes deployed in a geographic area.

104. The system of claim 95, wherein each site captures the notifications transmitted by a set of nodes, the set of nodes remaining unchanged.

105. The system of claim 95, wherein the plurality of sites comprises two portions, wherein a first portion includes sites configured to communicate with any other site in the first portion, wherein a second portion includes at least one site configured to communicate with only one site in the first portion, and wherein the system further comprises:

means for capturing, on a site in the second portion, an indication of the notifications captured by the site;

means for transferring, to a site in the first portion, the indication captured by the means for capturing.

106. The system of claim 105, further comprising:

means for transferring the indication received at the site in the first portion to another site in the first portion.

107. The system of claim 105, wherein the means for transferring transfers the indication after a predetermined period of time elapses.

108. The system of claim 105, wherein the means for transferring transfers the indication upon a notification captured by the site in the second portion satisfying a predetermined criterion.